Ring-LWE: A number theorist's perspective

joint with
(Yara Elias, Kristin E. Lauter, and Ekin Ozman)
and
(Hao Chen and Kristin E. Lauter)

SaTC, June 16th, 2016

Learning with errors

Let q be prime, n a positive integer.

Problem: Find a secret $s \in \mathbb{F}_q^n$ given a linear system that s approximately solves.

- Gaussian elimination amplifies the 'errors', fails to solve the problem.

In other words, find $s \in (\mathbb{Z}/q\mathbb{Z})^n$ given multiple samples

$$(a, \langle a, s \rangle + e) \in (\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{R}/q\mathbb{Z}$$

where e is chosen from an error distribution χ on $\mathbb{R}$.

Toward Ring-LWE

- Replace $(\mathbb{Z}/q\mathbb{Z})^n$ with a ring R_q
- Replace $\langle a, s \rangle$ with $a \cdot s$ (ring multiplication)

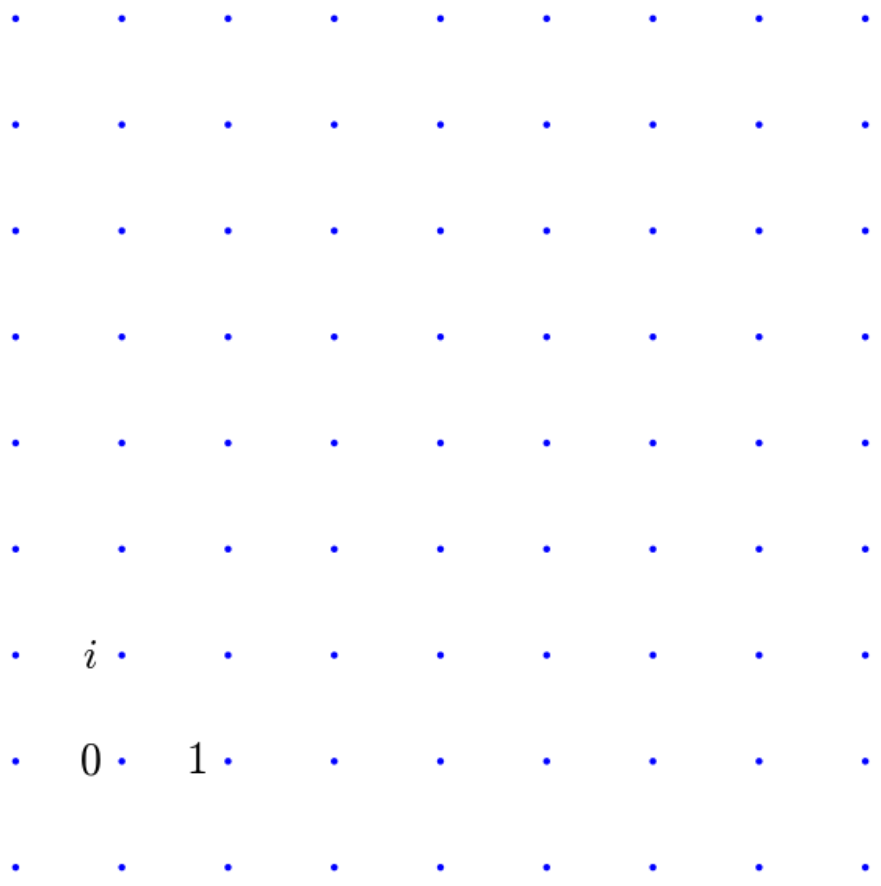
Search Ring-LWE: Find $s \in R_q$ given samples

$$(a, as + e) \in R_q \times R_q$$

where $a \in R_q$ is uniform and $e \in R_q$ is taken according to an error distribution χ

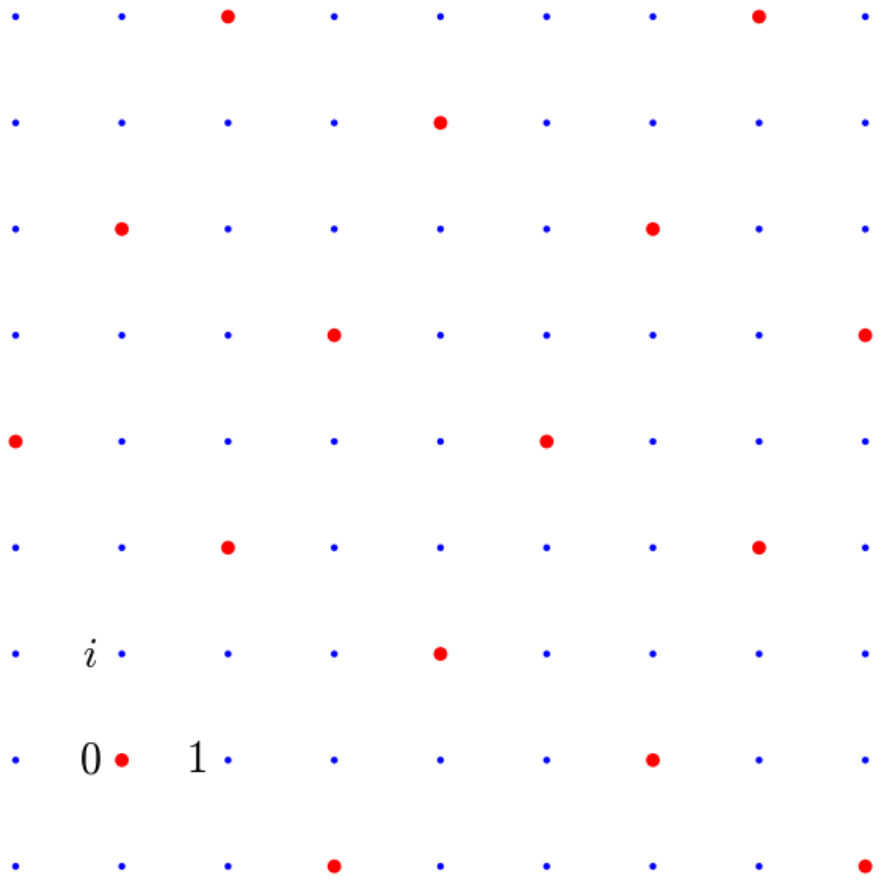
Decision Ring-LWE: Given samples in $R_q \times R_q$, determine if they are Ring-LWE samples or uniformly chosen.

Rings of Integers: example $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$



Multiplication by $r \in R$ is a linear transformation $L \to L$, $x \mapsto rx$.

Rings of Integers: example $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$



An *ideal* is a sublattice $I \subset R$ such that $R \cdot I = I$.

Discrete vs. continuous

We may wish to form a vector space $K_{\mathbb{R}} = R \otimes_{\mathbb{Z}} \mathbb{R}$ containing R and allow errors to be chosen there.

So, find $s \in R_q$ given samples

$$(a, as + e) \in R_q \times K_{\mathbb{R}}/qR$$

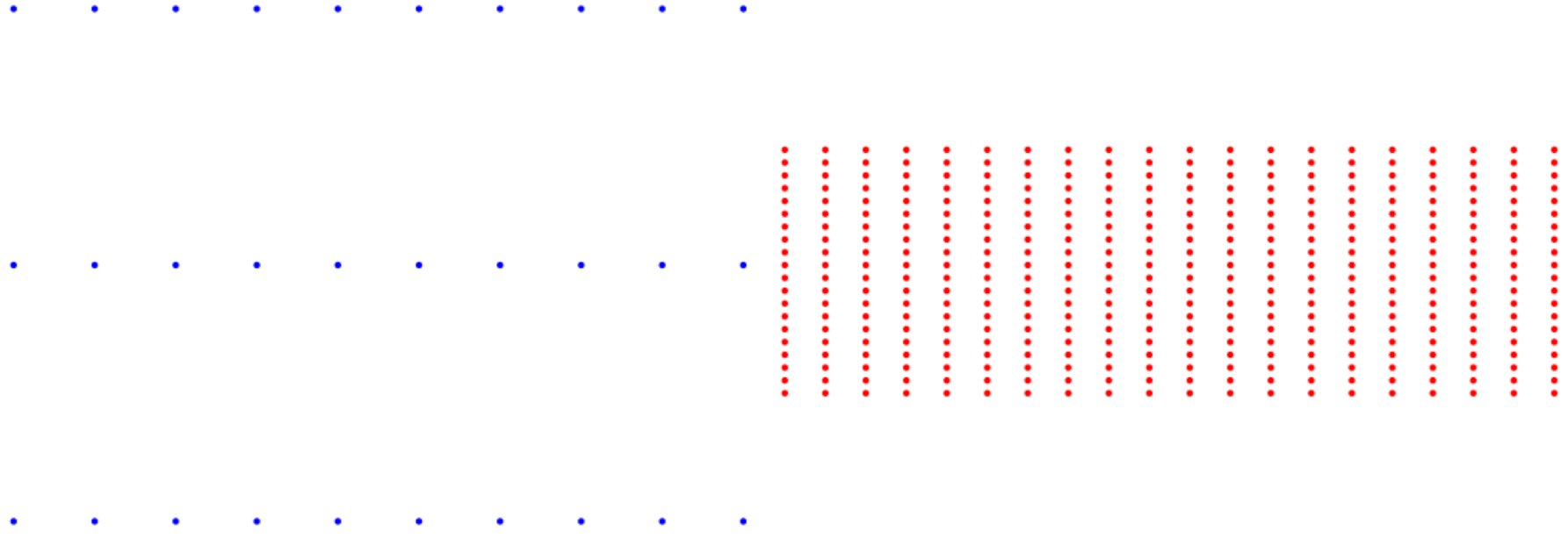
where $a \in R_q$ is uniform and $e \in K_{\mathbb{R}}$ is taken according to an error distribution χ

If one can solve discrete, then one can solve continuous, by rounding the continous samples.

Discrete is practical.

Dual lattices

$$L^\vee = \{v : \langle v, L \rangle \in \mathbb{Z}\}$$



Lattice

Dual

Dual vs. non-dual

We may wish to allow s, e to live in the dual lattice $R^\vee$ (so $R_q^\vee = R^\vee / qR^\vee$).

So, find $s \in R_q^\vee$ given samples

$$(a, as + e) \in R_q \times R_q^\vee$$

where $a \in R_q$ is uniform and $e \in R_q^\vee$ is taken according to an error distribution χ.

These are equivalent by a change of error distribution.

Error distribution

The error distribution is usually *Gaussian around the origin*:

$$\rho_r(\mathbf{x}) = \exp(-\pi\langle \mathbf{x}, \mathbf{x}\rangle / r^2).$$

Need an *inner product*.

- **Polynomial embedding** If $K = \mathbb{Q}[x]/(f(x))$, use

$$K \hookrightarrow \mathbb{R}^n, \quad a_n x^n + \ldots + a_0 \mapsto (a_n, \ldots, a_0).$$

  then use the standard inner product.
- **Minkowski embedding** Use trace pairing:

$$\langle a, b\rangle = \mathrm{tr}(ab) \in \mathbb{Q}, \quad a, b \in K.$$

- R **vs.** $R^\vee$

The difference is a linear transformation – spherical Gaussian in one is ellipsoidal in another.

Setting parameters

- n, dimension
- q, prime
  - q polynomial in n (security, usability)
- R, ring of integers
  - 2-power cyclotomics
  - other cyclotomics
  - other rings
- χ, error distribution, Gaussian, standard deviation σ
  - polynomial dual in practice
  - minkowski dual in theory
  - 2-power cyclotomics. Up to scaling/rotation:
    poly dual = mink dual = poly non-dual = mink non-dual

Example: $n \approx 2^{10}, \quad q \approx 2^{31}, \quad \sigma \approx 8$

Attack on Decision RLWE for (discrete non-dual) polynomial-embedding

(Eisenträger, Hallgren and Lauter)

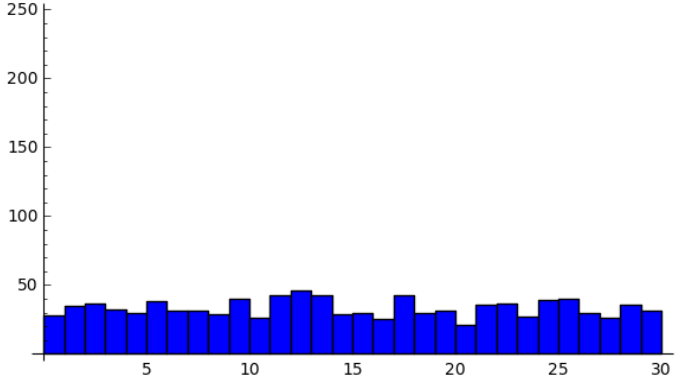
$$R = \mathbb{Z}[x]/(f(x))$$

potential weakness: $f(1) \equiv 0$ **mod** q**.**

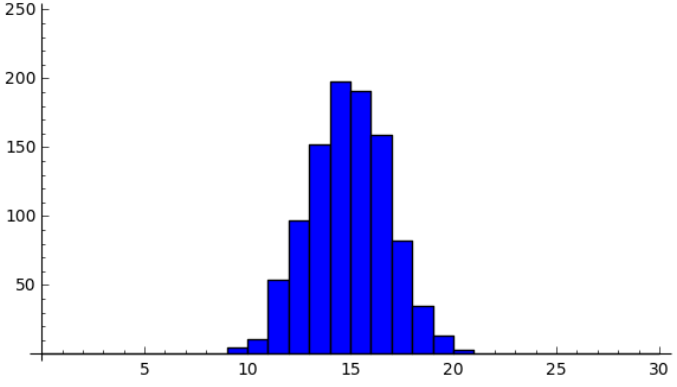
$$R_q \xrightarrow[\text{ring homomorphism}]{\text{evaluation at 1}} \mathbb{F}_q$$

$$(a, b = as + e) \longmapsto (a(1), b(1) = a(1)s(1) + e(1))$$

Guess $s(1) = g$, graph supposed errors $b(1) - a(1)g$:



Incorrect



Correct

Abstracting the key idea

If $\mathfrak{q}$ is a prime above qR, then we have a **ring homomorphism**

$$\phi : R_q = R/(q) \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}.$$

This preserves the structure of samples:

$$(a, as + e) \mapsto (\phi(a), \phi(a)\phi(s) + \phi(e))$$

Possibly weak if

1. image space is **small** enough to search
2. error distribution is **non-uniform** after ϕ

Attack:

1. Loop through $g \in \mathbb{F}_{q^f}$ for putative $\phi(s)$
2. Test distribution of $\phi(b) - \phi(a)g$ (putative $\phi(e)$) on available samples.

Search-to-decision

$$\begin{array}{ccccccc} K & & R & & \mathfrak{q}_1 \cdots \mathfrak{q}_g = qR & & R/\mathfrak{q}R & & \cong \mathbb{F}_{q^f} \\ | n & & | & & | & & | & & | f \\ \mathbb{Q} & & \mathbb{Z} & & q & & \mathbb{Z}/q\mathbb{Z} & & \cong \mathbb{F}_q \end{array}$$

$$R/qR \to R/\mathfrak{q}R$$

- Our attacks recover $\phi(s)$, i.e., the secret modulo $\mathfrak{q}$. That is, it solves *Search-RLWE-*$\mathfrak{q}$.

Proposition (Eisenträger-Hallgren-Lauter, Chen-Lauter-S.)

Suppose $K/\mathbb{Q}$ is Galois of degree n, and $\mathfrak{q}$ a prime of residual degree f. Suppose there is an oracle which solves Search-RLWE-$\mathfrak{q}$. Then by n/f calls to the oracle, it is possible to solve Search-RLWE.

In practice

There are instances where

1. error is large enough so generic LWE attacks do not apply
2. error is smaller than security reductions require
3. these attacks apply

- $\mathfrak{q}$ **of degree** 1 **(**$\to \mathbb{F}_q$**):** $\mathbb{Z}[x]/(f(x))$ with $f(x) = x^n + q - 1$.
- $\mathfrak{q}$ **of degree** 2 **(**$\to \mathbb{F}_{q^2}$**):** $\mathbb{Q}(\zeta_p, \sqrt{d})$.
- **ramified prime in prime cyclotomic case.**

What's going on?

The key is the geometry of the lattices $\mathfrak{q} \subset R$.
Perspective 1: The shortest vectors of R either:

- coincide frequently modulo $\mathfrak{q}$, or
- lie frequently in a subfield modulo $\mathfrak{q}$

Perspective 2 (Peikert): The non-uniformity appears in the image of some $R_q \to \mathbb{F}_q$, i.e. there is a short vector in $\mathfrak{q}^\vee \setminus R^\vee$.

Security of an instance of Ring-LWE

- Fixing R and q, there is a finite list of homomorphisms.
- Therefore, to be assured of immunity of an instance of RLWE to this family of attacks, need only check that finitely many distributions look uniform!

Degree 2 is as fast as Degree 1 (Chen-Lauter-S.)

Setup:

- $\phi : R_q \to R/\mathfrak{q}$, residue degree 2
- image of error distribution lies in $\mathbb{F}_q$ with probability distinguishable from $1/q$

Idea: a and b in sample $(a, b = as + e)$ should correlate if errors are in subfield unusually often.

- $t_1, \ldots, t_q$ coset representatives of $\mathbb{F}_{q^2}/\mathbb{F}_q$
- Suppose $\phi(s) = s_0 + t_i$
- For sample (a, b), write $m_j(a, b) := \frac{b^q - b - (at_j)^q + at_j}{a^q - a} \in \mathbb{F}_q$
- If $j \neq i$, $m_j(a, b)$ look uniform
- If $j = i$, get $m_j(a, b) = s_0 + \frac{e^q - e}{a^q - a}$, has a peak at s_0

Attack: Loop through j, checking distribution

Conclusions

- The structure inherent in rings **is** exploitable
- The vulnerability has **sensitive dependence** on parameters
  - properties of the ring
  - properties of q (not just size)
  - properties of the error distribution

Open Problems

- What number theoretical properties of R or its ideals determine the length of the shortest vectors?
- Similarly, for dual lattices?
- Geometrically, how does $\mathfrak{q}$ sit inside R?
  - Short vectors in $\mathfrak{q}^\vee \setminus R^\vee$?
  - How do the shortest vectors of R distribute among cosets of $R/\mathfrak{q}$?
  - How do the cosets of $\mathfrak{q}$ corresponding to a subfield appear geometrically?
- If we see non-uniformity modulo $\mathfrak{q}$, what types of non-uniformity are allowed?